UNIVERSITY OF SOUTH DAKOTA

Policy Number: 2.041
Originating Office: Financial Affairs
Responsible Executive: VP of Financial Affairs
Date Issued: 09/24/2012
Date Last Revised: 10/01/2013

Credit Card Acceptance

Policy Contents

I. REASON FOR THIS POLICY

The University of South Dakota supports the acceptance of credit cards as payment for goods and services to improve customer service, bring efficiencies to the university's cash collection process, and increase the sales volume of certain types of transactions. In addition, the university must support unit compliance with industry standards governing credit card transactions processing, specifically Payment Card Instruct Data Security Standards (PCI DSS).

Many departments on campus process credit card transactions. It is the University of South Dakota's responsibility to protect the privacy of its customers, as well as maintain compliance with the Gramm Leach Bliley (GLB) Act and Payment Card Industry (PCI) Standards.

All University of South Dakota departments and colleges that conduct electronic-based financial transactions for the University of South Dakota, which include credit/debit card or electronic checks (eChecks) transactions, must be compliant with: Payment Card Industry Data Security Standards (PCI DSS), all applicable laws and mandates, and the South Dakota Board of Regents and USD policies and procedures. Failure to be compliant in all areas may result in the revocation of department authorization to accept electronic-based financial transactions and departmental responsibility for paying all related penalties. Currently, PCI DSS only applies to credit card transactions.

Departments must obtain prior approval to accept electronic-based financial transactions. Requests should be submitted to The University of South Dakota Comptroller.

Credit cards for current student accounts receivable payments are only accepted online via SDePay via NelNet Business Solutions. The University of South Dakota Business Office may process payments made by federal agencies and student accounts in collection.

II. STATEMENT OF POLICY

The University of South Dakota expects all units that accept credit cards to do so only in compliance with credit card industry standards, and in accordance with the procedures outlined in this document.

Departments must remain compliant with Payment Card Industry Data Security Standards (PCI DSS), all applicable laws and mandates, and South Dakota Board of Regent and USD policy and procedures.

If a department suspects that credit card records may have been compromised in any way, whether through malicious intent or due to a weakness in the handling and processing of credit card transactions, they are to notify the USD PCI Compliance Officer immediately. All security incidents will follow the USD Incident Response Policy.

In order to accept credit cards online for goods or services, departments must first be approved by the USD PCI Compliance Office and the USD Information & Technology Department. Acceptable credit cards include MasterCard, VISA, Discover, and American Express.

Staff access to cardholder system components and data is limited to only those individuals whose jobs require such access. Access rights for privileged user IDs is restricted to the least privileges necessary to perform job responsibilities. Privileges are assigned to individuals based on job classification and function.

Credit card information shall not be sent via e-mail or other unsecured communication methods (chat, instant messaging, etc.) nor stored on any form of media such as a computer, flash drive, external hard-drive, etc.

Hard copied Materials

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. Any forms containing cardholder information must be held in secure storage.

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include:

Media must be classified so the sensitivity of the data can be determined.

Media must be sent by a secure carrier or other delivery method that can be accurately tracked.

Logs must be maintained to track all media that is moved from a secured area, and management approval must be obtained prior to moving the media.

Strict control must be maintained over the storage and accessibility of media containing cardholder data.

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons.

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. Containers storing information waiting to be destroyed must be secured to prevent access to the contents. All forms will be designed so that any credit card information can be easily cut off after processing and shredded.

If it is necessary for staff to accept credit card information over the phone, the information is to be written on a piece of paper and hand-delivered to the appropriate office for processing. The paper containing the credit card information will be held in secure storage until the transaction is verified. It will then continue to be held in secure storage until it is shredded.

Credit card information may be faxed to an office. However, the fax machine must be in a secure area. Faxed information must be immediately hand delivered to the appropriate office for processing. Any electronic memory on fax/scanning machines used to disseminate credit card information must be fully erased or physically destroyed when the equipment is retired.

Terminals and underlying applications must be configured to mask the PAN when displayed.

The security code will not be requested for any transaction unless through an authorized third party service provider.

All terminals and underlying systems must be configured to truncate account numbers on printed copies of receipts.

Recurring payments will be handled by the credit card service provider and will not require access to the PAN by USD staff.

III. DEFINITIONS

FOAP – Banner Fund, Organization, Account Code and Program

DEPARTMENT - A USD department that accepts credit cards to conduct business.

ELECTRONIC FUNDS TRANSACTION - The term is used for a number of different concepts, such as cardholder-initiated transactions, where a cardholder makes use of a payment card (e.g., credit or debit card); electronic payments by businesses, individuals, or students, using electronic check clearing (banking information).

GRAMM LEACH BLILEY ACT - Key rules under the Act govern the collection and disclosure of customers' personal financial information.

PAYMENT CARD INDUSTRY (PCI) STANDARDS - A multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. For more information, visit https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

CAV2, CVC2, CID, OR CVV2 DATA - are the three-or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

PIN DATA - is the personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transactions message.

IV. PROCEDURES

Obtaining Authorization to Accept Credit Card Payments

Departments must obtain prior approval from The University of South Dakota Comptroller to accept and/or process credit card transactions. An email request must be returned to the Comptroller. If approved, the Comptroller along with ITS will assist the department in obtaining the required information and equipment needed to process credit card transactions. The Business Office will assist in providing the department with procedures for processing credit card deposits and reconciling them daily. If a department has not obtained approval to accept and process credit card payments, they should not be accepting credit card information.

Departments must ensure that procedures are followed, and PCI Data Security Standards are met. Access to system components, banking information, and cardholder data should be limited to only those individuals whose jobs require such access. Departments are responsible for providing their employees with policies and procedures to ensure compliance with PCI Data Security Standards and USD policies and procedures.

All paper and electronic media that contain cardholder data should be physically secure and confidential. All cardholder data should be disposed

of according to records retention policy and PCI Data Security Standards. Documents should be cross-cut shredded or incinerated so that cardholder data or financial information cannot be reconstructed.

Methods of Processing Methods of Processing Transactions

The acceptable methods for processing credit card transactions include:

1. in person.
2. By telephone – if the CVV code is obtained from the back of the card, it must be destroyed after the transaction is processed; must verify the address if sending merchandise; may choose to have return receipt to confirm delivery of goods.
3. By fax – only if fax machine is in a secure, limited access location, accessible only by authorized personnel.
4. By mail – this is not the preferred method. All documents containing cardholder data must be secure and disposed of according to records retention and PCI Data Security Standards. No storage of magnetic stripe data, CVV, PIN, or other similar information may be retained.

Credit card information must not be requested or sent electronically (i.e. email, instant messaging). If the cardholder sends credit card information electronically, departments cannot process the transaction. The department must delete electronic communication immediately. The department must notify the customer that USD does not accept credit card information electronically. The information can be provided over the phone or by mail if necessary.

The following information should be sent or communicated with the customer:

It is important that USD protects the privacy of our customers, and therefore, does not accept credit card information electronically, as the email system is not a secure site. Please discontinue sending credit card information electronically. Please contact the department providing the goods or services to request available payment options.

When issuing credits to customers, the credit should be processed in the same payment method as the original charge. The department must contact the USD Business Office with the transaction identification. Exceptions should be approved by the departmental head/manager on a case-by-case basis.

Departments must not store any credit card information, including CVV codes or PIN numbers, in a customer database or electronic spreadsheet. All CVV codes, PIN numbers, and other documents containing credit card information must be shredded immediately after the transaction has been processed. It is violated by PCI Data Security Standards to store magnetic stripe (i.e. track) data, CAV2, CVC2, CID, or CVV2 data, or PIN data after transaction authorization on any systems**.**

Magnetic strip data is data encoded in the magnetic stripe used for authorization during a card- present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements

of track data that may be retained are account number, expiration date, and name.

Refunds

When an item or service is purchased using a credit card, and a refund is necessary, the refund should be credited to the credit card from which the purchase was made. The department must contact the USD Business Office with the transaction id. Exceptions should be approved by the departmental head/manager on a case-by-case basis.

Disputed Charges / Chargebacks

Occasionally, the credit card processor will send notification to the university indicating a disputed charge. A copy of this chargeback notification will be investigated by the Accounting Department. If necessary, the department is required to provide all requested information in response to the notification by the due date indicated. Failure to provide the requested information in a timely manner will result in the department being charged for the transaction in question and the department cannot appeal the chargeback.

Recording and Reconciling Credit Card Transactions

The department must complete a daily deposit advice form for all credit card transactions and deliver the following information to the USD Business Office.

1. **Daily Totals Report** - this includes only the totals for MasterCard, VISA, Discover, and American Express; no credit card numbers are included.
2. **Daily Settlement Report** - this indicates the amount settled successfully; no credit card numbers are included. - Departments should transmit and settle their batches daily.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Not Applicable.